REMARKS

These remarks are set forth in response to the non-final office action mailed Septmeber 28, 2004 (the "Office Action"). As this amendment has been timely filed within the three-month statutory period, neither an extension of time nor a fee is required. Presently, claims 1 through 16 are pending in the Patent Application. In the Office Action, each of claims 1 through 16 have been rejected under 35 U.S.C. §102(e) as being anticipated by United States Patent No. 6,,754,714 to Chebrolu issued on June 22, 2004. Additionally, claims 1, 5, 9 and 13 have been rejected under 35 U.S.C. §102(e) as being anticipated by the publication Pars Mutaf, *Defending against a Denial-of-Service Attack on TCP*, International Symposium on Recent Advances in Intrusion Detection (Purdue 1999)(Mutaf).

Chebrolu relates to a multilink point-to-point protocol network access server channel allocation method and apparatus. Specifically, Chebrolu addresses the problem of ensuring that subscribers to an Internet Service Provider (ISP) can establish a connection with a network access server despite a limited availability of channels over which a connection can be made with the ISP. To achieve the foregoing, secondary "back channels" which provide a supplemental pipe for downloading data can be used to provide ISP access to subscribers when no more primary channels are available.

Notwithstanding, Chebrolu does not address the problem of defending against network connection flooding attacks. Rather, Chebrolu relates exclusively to an attempt to *facilitate* the establishment of a connection as compared to the *denial* of an attempt to establish a connection. In fact, nowhere in Chebrolu is it ever suggested that a network flooding attack can be detected and processed. Rather, at best Chebrolu mentions that "customer service" can be adversely

affected "when a user/client's request for an ISP connection is denied due to lack of allocable channel capacity".

In reference to the specifically cited portions of Chebrolu, column 1, lines 15-30 speak only to the allocation of a secondary channel in a network access system to increase download bandwidth and that if "all available channels on a given network access system are allocated among various users, then no new users can obtain access because there is not available channel." Column 2, lines 20-25 states in its entirety, "For the sake of simplicity in FIG. 1 (and in similarly arranged FIG. 2), a given client is shown connected with a given ISP, but it will be understood that a single client typically may be connected with any one or more of plural ISPs and that any one or more of plural clients may be connected with a single ISP." Hence, it is clear that the cited portions of Chebrolu have nothing to do with defending against network connection flooding attacks.

Mutaf, unlike Chebrolu, speaks directly to a flooding attack in the form of a Denial-of-Service (DoS) attack. Specifically, Mutaf teaches a real-time anomaly detection method for detecting TCP SYN flooding attacks. The methodology of Mutaf is based on the intensities of SYN segments which are measured on a network monitoring machine, in real-time. Specifically, in Mutaf, in order to determine the actual level of threat faced by an attack, a series of host based measures can be provided--namely tuning the TCP backlog queue lengths of exposed servers.

At any rate, the cited portion of Mutaf on page 6 relates specifically to the detection method which can account for three parameters associated with a SYN flooding attack: a timeout value, a per-port backlog queue length and a number of received SYN segments per second per port which essentially is a rate metric. Where the rate of received SYN segments per

second per port exceeds a threshold rate, then an attack can be determined to be underway and the queue length and timeout value can be adjusted accordingly. Significantly, nowhere in Mutaf is it ever suggested that a connection can be denied. In fact, the very nature of a SYN flood attack is to never complete a connection, but to merely flood a device with "half-open" connections.

In summary, the teachings of each of Chebrolu and Mutaf are not sufficient to support the rejection of any of claims 1 through 16. In particular, Chebrolu literally bears no relation to detecting a flooding attack and denying a connection, while Mutaf never engages in the denial of a connection based upon a flooding attack detection. Rather, in Mutaf only queue lengths and timeout values are adjusted.

For all of the above reasons, the claim objections are believed to have been overcome placing Claims 1 through 16 in condition for allowance, and reconsideration and allowance thereof is respectfully requested. Additionally, to facilitate the reconsideration of the application of the Chebrolu and Mutaf references to claims 1 through 16, the Applicants further request an on-site, personal interview with the Examiner. In the interim, the Examiner is encouraged to telephone the undersigned to discuss any matter that would expedite allowance of the present application.

Respectfully submitted,

Date: December 27, 2004

Steven M. Greenberg
CUSTOMER NUMBER 46320

16058